

REMARKS/ARGUMENTS

Claims 1-25 stand in the present application. Reconsideration and favorable action is respectfully requested in view of the following remarks.

In the Office Action, the Examiner has rejected all of claims 1-25 under 35 U.S.C. § 102(b) as being anticipated by Kambayashi et al. (hereinafter "Kambayashi").

Applicant respectfully traverses the rejection.

The Examiner alleges that claim 1 feature "(a) keys encrypting a plurality of data units each with one of a sequence of keys" is disclosed in the cited reference. Applicant respectfully disagrees.

Nowhere does Kambayashi teach or even suggest a sequence of encryption keys, one per unit of information. Figures 111-140 cited by the Examiner do not show this feature, nor does any other figure or text of Kambayashi show or disclose this feature. There are two levels at which the examiner could have possibly mistakenly perceived Kambayashi was using a sequence of keys, one per unit of information:

- i) encryption of the content information
- ii) encryption of the license information

However, as explained below, both are incorrect.

The following citations describe the way all five embodiments in Kambayashi work.

Col 4, lines 32-55

Col 40, line 60 - col. 41, line 33

Figs. 55-69.

i) Content information is encrypted with a single key:

All five embodiments described in the Kambayashi patent rely on the information reproduction equipment being trusted by the content owner. Content information is encrypted with a single key (K1). The content owner can only discriminate access to different parts of the content by describing in the license info which parts of the content should be accessible and when. Once the reproduction equipment has extracted K1 it could access all of the content information, but instead the content owner trusts it to only give the user access to the parts of the information that are defined in the license information.

ii) license information is also encrypted with a single key:

See for instance Fig. 66 or Fig. 114 of Kambayashi, where the license info is encrypted with one common or public key respectively.

The Examiner has also mistakenly alleged that claim 1 feature “(d) generating from the seed values a sequence of keys greater in number than the number of seed values communicated to the user terminal” is disclosed in the cited reference.

Kambayashi doesn't achieve the feat of generating more keys from less seeds.

In rejecting the claims on the basis the Examiner again cites Figs. 111-140 (and more specifically the subset of Figs. 134-138 in some cases). In no case does the Examiner cite to any text. Figs. 111-140 show two embodiments, the fourth embodiment at Figs. 107-121 and the fifth embodiment at Figs. 122-140 (and onward). So this is an extremely broad citation pointing to nearly all of two whole embodiments of the system. If it were not for the Examiner's more specific citation of Figs. 134-138, it would be difficult to know exactly what the rejection was based on, as Kambayashi's system is not similar in any way to Applicant's.

Kambayashi's patent is an extremely simple (and incredibly naive) solution dressed up in layer upon layer of complex language and flow diagrams. Essentially, every player is manufactured with a disk contents key embedded in it and presumably relies on tamper-resistant to prevent this key being leaked (though this is not admitted).

The player is trusted to comply with any correctly encrypted license condition given to it (e.g., the dates it will allow playing a disk to occur and in which player it is allowed). But this license condition must be transferred securely from the license issuing center to the player using a correct key.

All the key exchanges repeated throughout the patent are merely to ensure that it is not possible to eavesdrop the keys used to transfer the license information from the license issuing device to the player (via the card and the two card adapters in the shop and in the user's player). If these transfers were not secure, someone could fake an open license condition and sign it and feed it into the trusted player to make it play whatever they wanted.

In focusing on Figs. 134-138, which are the most specific items that the Examiner cites against the present claims, we find these figures show six sub-processes of the fifth embodiment that are all actually identical in that they result in agreeing a key between various pairs of modules in the system. Each sub-process use the standard Diffie-Hellman key agreement protocol in six different instances, described in the text starting on line 6, col. 79, summarized in Fig. 133, and listed below, where the following abbreviations for different parts of the system are used:

L: License issuing device

A: card Adapter

P: card

D: Player

Fig. 134/6 agreeing S2 between L & A using two pre-shared secrets, XI, PrI

Fig. 135 agreeing S1 between L & P using two pre-shared secrets, Xk, Prk

Fig. 136 agreeing S3 between L & A using two pre-shared secrets, XI, PrI

Fig. 137 agreeing S4 between A & D using two pre-shared secrets, XD, PrD

Fig. 138 agreeing S6 between D & A using two pre-shared secrets, XD, PrD

Fig. 139 agreeing S5 between P & A using two pre-shared secrets, Xk, Prk

Each of the six seeds, S1-S6, are used to generate a shared key between the stated pair of modules using a pre-stored algorithm in both. So six pre-shared secrets, XI PrI Xk Prk XD PrD, are used to create six seeds, which in turn are used to create six shared keys. So Kambayashi is not generating more keys than the original number of seeds, nor more than the original number of pre-shared secrets.

However, even if Kambayashi "might" have generated more than six keys from these six secrets by multiple iterated uses of Kambayashi's system, the important point is that these would not be a "sequence" of keys. Each time the Diffie-Hellman protocol is invoked, two different random numbers are generated by the two devices in order to agree a new key based on the two pre-shared secrets and the random numbers. The point of Diffie-Hellman is that each key that it generates is random, but known between the two devices. On the other hand, Applicant's invention involves the generation of a pseudo-random "sequence" of keys. Because it is a sequence, the same sequence can

be consistently re-generated from the same seeds.

Moreover, Applicant's invention is more than simply generating a pseudo-random sequences of keys. A key feature of Applicant's invention is generally an "arbitrarily doubly bounded portion of the sequence" "greater than the number of seeds." See claim 1 at (d) and (e) wherein a sequence of keys constituting an arbitrarily doubly bounded portion of the sequence of keys of step (a) is generated.

The Examiner states that Kambayashi clearly generates "a subset of the entire key space." (See Office Action at page 4.) That's as may be. But a subset is not a sequence, let alone a bounded portion of the sequence, let alone doubly bounded, let alone arbitrarily doubly bounded, as required by the present claims.

Therefore, in view of the above remarks, it is respectfully requested that the application be reconsidered and that all of claims 1-25, standing in the application, be allowed and that the case be passed to issue. If there are any other issues remaining which the Examiner believes could be resolved through either a supplemental response or an Examiner's amendment, the Examiner is respectfully requested to contact the undersigned at the local telephone exchange indicated below.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

Chris Comuntzis
Reg. No. 31,097

CC:Imr
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100